TOrBAC: A Trust Organization Based Access Control Model for Cloud Computing Systems

Mustapha Ben Saidi, Anas Abou Elkalam, Abderrahim Marzouk

Abstract--The access control models like DAC, MAC, RBAC, TBAC, TMAC, DomBAC, etc. mainly model security policies for information systems having a centralized governance. Moreover, they only specify permissions and prohibitions, sometimes obligations. Besides that, they generally do not allow the establishment of activated, dynamic and adapted rules. However, such rules are highly useful in a cloud environment where IT governance is shared, used or managed by different entities. In this paper, we propose a new model for specifying such security policies. This model called Trust Organization Based Access Control (TOrBAC) which relies on the use of a recursive formula for calculating a confidence index. We also formalize our work using a language based on first order logic and we apply it to a cloud computing (CC) related use case.

Keywords: Cloud computing; Access model control; security.

I. INTRODUCTION

Cloud computing is a general concept that incorporates internet based (cloud) development, use and storage of computer technology. For example Google Apps, provides common business applications online that are accessed from a web browser, while the software and date are stored on the servers and cached temporarily on clients, tablet computers, notebooks, wall computers handles, sensors, monitors etc. In this context, as more and more information on individuals and companies is placed in the cloud while the Cloud is actually a fairly new and emergent technology with several open areas mainly related to security: remote storage, data dispersion, multi-location, isolation, risk exposure, data lost, abuse and malicious use, non-secure API, account or service diversion, etc.

Privacy, trust and access control are hence some of the most important security concepts met in Cloud systems.

In particular, access control is of vital importance in a Cloud environment since it is concerned with allowing a user to access a number of Cloud resources: wh has access to what, when, how and under which conditions? An extensive research has been done in the area of access control in collaborative systems but few works are really dedicated to the cloud computing. Further examination is thus necessary, especially duo to this domain specificities and to the partial or weak fulfilment of security requirements in the Cloud.

Manuscript received September 02, 2012.

Mustapha Ben Saidi Lab. MAI. FST Settat University Hassan 1 Settat Morocco.

Anas Abou Elkalam Cadi ayyad University, ENSAof Marrakech, OSCARS laboratory, Marrakech Morocco.

Abderrahim Marzouk Lab MAI. FST University Hassan 1er Settat Morocco.

More precisely, classical access control models such as RBAC [6], TBAC [5], DomBAC [4]; PolyBAC [3], OrBAC [1] have clear limitations in a cloud environment [12]. Up to our knowledge, none of these models can overcome the following requirements identified by all stakeholders of Cloud Computing (CC) [10]:

- Rules that specify permissions conditioned by a degree of confidence. For example, a virtual cell of doctors has special permissions in a cloud environment (universal virtual emergency for example) conditioned by a definite confidence index.
- Rules that manage the convergence of permissions to prohibitions (what we call 0-recommendations in this paper) based on the deterioration of the confidence index.
- Rules of trust management in real time, and assigned confidence index or value.

The concept of trust is actually central in this new model. Basically, the degree of confidence is an index on which pivot the majority of safety and regulations; so that it is possible to manage in real time several security policies associated with the dynamic level of the Confidence Index. Our model extends the concepts of permission, obligation, prohibition and Recommendations [2, 9] to P-Recommendation with 0 <= P (weight) <= 1, which is the largest model.

Dedicated to the cloud access control, this paper is organized as follows: Section 2 presents the current state of access control models based on roles, organizations and contexts as well as their limitations in cloud computing environment (CC). In Section 3 we present an overview of our idea. Then, Section 4 presents our model TOrBAC (T*rust Organization-Based Access Control*) based on the trust management in the CC environment. Afterwards, we define a language based on first order logic that we use to model a "TorBAC" security policy. We then apply our work to a case in the medical field. Finally, Section 5 concludes the paper and presents some perspectives.

II. CLOUD COMPUTING

A. Define and understand cloud computing

Since the beginning of the computer industry, the large-scale distributed computing has always been a dream gradually reached; its realization has also started with the grid technology computing "grid computing", which are to become flat ideal platforms for researchers of any discipline. The dream continues to dig open the appetite to exploit this technology in the management information systems of companies. Quickly after a few years of its appearance, grids give birth to a massive wide consumer technology.

It is therefore technology rental demand services from which the company buys the license. These services are generally available from providers who are on an environment that is called cloud computing. Many people mistakenly believe that cloud computing is nothing more than the Internet under a different name. Many designs of systems based on web services represent the Internet as a cloud, and people refer to applications running on the Internet as "run in the cloud", so the confusion is understandable. The Internet has many features in common with what we now call cloud computing. The Internet provides the abstraction runs using the same set of protocols and standards and uses the same applications and operating systems. When an intranet is large enough and its architecture is independent of the person's physical systems, intranet can be identified with a cloud or "cloud computing CC" private. [16]

Cloud infrastructure is based on three axes:

High flow networks: networks are increasingly free to the son and soon gigabits Gbit / S will be available. Therefore, 100Mbits / s will be trivialized. Generation 3G, LTE, Wi-Fi, Wi-MAX ... Good coverage of global networks is by appointment.

External servers: it is a set of servers together in "Public Cloud" or "Private Cloud" or "Cloud community," the company does not handle goal icts year service operator through Cloud. Dominance of Large Firms is very clear in this regard: Amazon, Google, IBM, Microsoft, ... This vast network of servers offer such computing power, storage space or a platform company uses when it needs it. [17] Access objects: all cloud applications should have the characteristics of a browser. The statistics say that by 2020 the world will be connected to mobile to 80%. This mobile is more powerful multi-network (use of next generation networks increase), have a variety of OS have multiple browsers, etc...

Cloud computing can be seen as an abstraction based on the concept of sharing of physical resources and presenting them as a virtual resource. It means that online resources are used as if they were located in the ether, in a space with no physical reality. Some players also play world of immateriality this: for example, Google maintains a mystery about the location of its data centers or Datacenter [10].

CC offers three types of services: services that use this software or SeaS "Software as a service", and technical services or PaaS and IaaS i.e. "Platform as a Service and Infrastructure as a Service."

SaaS:

This is to rent monthly or annual operational or more specifically applications without buying or installing or maintaining "Muti-taking." Thus, an operator can establish a contract to provide the company with one or more services that operate as needed. Therefore, it will pay only if it has consumed. An example in a company in need of AutoCAD to draw a single year plan, you will not need to buy a license for such a need, an operator may cloud to provide its subscriber rental instantaneous which will be much more economical. Among the operators in this sense are: Google apps, Microsoft, IBM Lotus Live, YouTube and daily motion, Google book search.... Some speak of access to the best applications in the world by everyone.

PaaS :

In this case, the service provides a platform for customized work (mostly developers); they can exploit, deduce from the results and then release the platform. The invoice will be issued by the service provider based on usage. For example, if a developer needed to update a function written in an IDE that he does not, he may appeal to the IDE with an operator. Among the major PaaS offerings in include Amazon Web Services, VMware vCloud...

IaaS :

Infrastructure as a Service is to make available to subscribers of storage space to host their site or set their databases. IaaS is the necessary infrastructure for SaaS and PaaS. So IaaS is essentially dedicated administrators SID companies that offer subscribers as Microsoft Azure infrastructure.

B. Cloud architecture

There are several cloud deployment models:

Public: External organization, accessible via the Internet, managed by an external service provider owns the infrastructure with resources shared between several companies.

Private: In this case, the system is hosted internally. It can be a "cloud" inside the DSI or dedicated cloud and accessible via secure networks, hosted by a third shared between different entities of a single company. Open to partners of the company (suppliers, consultants, key customers, financial institutions, service key ...) or a professional group.

Community: It allows multiple independent entities to enjoy the benefits of shared costs of a non-public cloud, while avoiding some security issues and regulations that may be associated with the use of a generic public cloud that had not responded to their concerns.

C. Security issue: Risk Analysis of Security in the Cloud

As each technological breakthrough, the "cloud computing" brings new risks that must be taken into account before you can enjoy all the benefits of the solution. When an organization migrates to a cloud service, especially public cloud services, much of its information is now under the control of a third party cloud service provider (CSP). This offset could exacerbate the problem of security and confidence to users.

Modification, deletion, and transmission of sensitive data outside the company, should be avoided by DSIS. They can deploy DLP (Data Leakage Protection) to achieve this goal even if these solutions are complex to deploy and configure. DLP tools should be used to detect any loss of data.

In addition, virtualization introduces the ability to copy a complete virtual image and share it between users, thus creating a new information leakage vector. Similarly, snapshot backups (snapshot), or other copies of volume must be protected. [17].

Management issues of compliance and risk management of identities and access, integrity and service endpoints and data protection must be considered in the evaluation, implementation, management and maintenance solutions "cloud computing." Although they offer many potential benefits, the services provided through the cloud can also create new problems, some of which are not yet fully understood. By adopting a cloud service, IT organizations must adapt for example the fact that data management is no longer under their direct control.

In addition, the study Easy net Global Services cited above also shows that more than a third (38%) information centers and orientation (CIO) European respondents believe that cloud induces risks relating to 'uptime' time from which a machine or computer software, running without interruption. "This therefore poses risks to availability (being ready to use) and reliability (continuity of service) [16].

But overall, we can identify the following risks when using the CC:

- Risk 1: Loss of control and / or governance
- Risk 2: Deficiencies at interfaces and APIs.
- Risk 3: Compliance (s) and maintain compliance: The protean context of cloud generates many issues related to regulatory and legal aspects including:
  - The responsibility of data and processes.
  - Cooperation with legal entities and justice (in different countries).
  - Traceability of access to data in the cloud as well, when the data is saved or archived.
  - The ability to perform inspections and audits on compliance procedures and procedures.
- Compliance with regulatory requirements trades.
- Risk 4: Location continuous data.
- Risk 5: Segregation / Isolation environments and data.
- Risk 6: Loss and destruction of controlled data
- Risk 7: Retrieving data.
- Risk 8: Malice in use.
- Risk 9: Impersonation when accessing data.

These questions may have answers in parts, some operators, but third trust actors who hold the information in the CC operator feed the majority of these risks. This sense of risk is primarily related to identity management key players, who represent the operator and hold information each company has opted for such a solution. These issues of trust and identity are not yet covered by the access control policies in the context of traditional Cloud. It is therefore necessary to combine other ideas what is the technique that is human namely "trust" which is variable in time and especially during access, which makes the control more. In this paper, we propose a solution in regard to.

III. SOME CLASSICAL ACCESS CONTROL MODELS

A. Access control based on roles: RBAC for Cloud

A Cloud access control policy can be defined as a Cloud security properties and rules that specifies how a user may access a specific resource and when. Such a policy can be enforced in a Cloud system through an access control mechanism. The latter is responsible for granting or denying a user access upon a resource. However, how to be sure that the security policy is consistent and compete? Are we sure that this policy is implemented by suitable security mechanisms? Etc. Answers to such questions require associating a security model to the policy. Basically, an access control model can be defined as an abstract container of a collection of access control mechanism implementations, which is capable of preserving support for the specification and reasoning of the system policies through a conceptual (and if possible, a mathematical or formal) framework. Somehow, the access control model help to formalize, be sure … and bridges the existing abstraction gap between the mechanism and the policy in a system.

Several access control models have been developed during the last decades, namely the Mandatory Access Control policies (MAC), the Discretionary Access Control policies (DAC) and the Role Based Access Control policies (RBAC). Each one of them serves specific security requirements in different working environments. Note that some research on the MAC, DAC and RBAC has proven that an access control model, which can express the role based access control policies, is also capable of enforcing both MAC and DAC policies [22]. Some extension of Or BAC like Or BAC (Organization-Based Access Control) and poly-OrBAC are morerich and cover the requirements of collaborative systems [23, 24]. In the rest of this section, we give an overview of this model.

In RBAC, the access rights are based on the notion of roles to which each user is associated, which makes the model more flexible and easier to manage and already has several benefits to extend it to include Cloud [8]:

- Facilitate the management of permissions.
- Facilitate the definition and role management.
- Facilitate the provision of fewer privileges.
- Facilitate the sharing of responsibilities.

However, this model has at least two limitations faced to the cloud computing environments: the first is a flexible and adaptable dynamic management of access rights, while the second concerns the management of accesses by different collaborative but independent organizations. This justifies the need to develop an extension to achieve these requirements.

B. Organization-Based Access control (OrBAC*)*

Centered on the organization, OrBAC (*Organization-Based Access* Control) uses the abstract concepts of role, purpose and activity group and structure for the subjects, objects and actions. It allows you to define security policy only abstract entities (regardless of the details of implementations in organizations) by assigning permissions, obligations, prohibitions and recommendations to roles to perform activities on views in a particular context. In this model, we define eight entities that interact using the model described in Figure.1 [7]:

- Subject: this refers to active entities to which we assign rights (users).
- Organization: somewhat be seen as a structured group of active entities, that is to say, subjects playing certain roles, e.g. accounting department.
- Role: is used to structure the relationship between individuals and organizations. In the context of cloud, the accounting role is played by users while the DBA service role is played by organizations.
- Object: represents mainly non-active entities such as files, emails, printed forms, etc.
- Action: mainly includes computer concrete actions as select », « openfile () », «send » etc.
- View: set of objects that satisfy a common property, e.g. in a cloud, the view "administrative records" covers all administrative records of a client. The same view can be defined in an enterprise as a set of Word documents.

- Activity: corresponds to actions that have a common goal. Example: "consult", "edit", "pass", etc. The activity "consult" may amount, in the hospital organization action "read" a file, but can just as easily correspond to the action "select" on a database in another organization
- Context: used to express circumstances such as: normal, emergency, "computer abuse," "intrusion". Context can also consider the temporal aspects (access time) special (address from which the query originates) access history, etc.

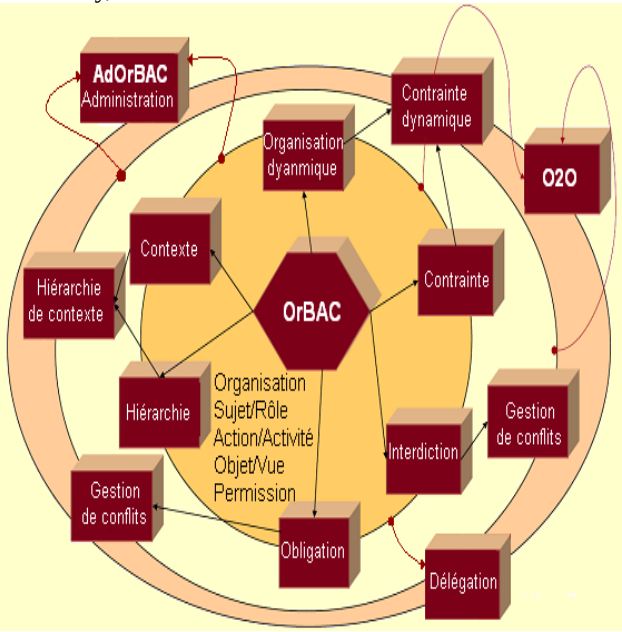


Fig. 1: Extension du modèle OrBAC [7]

C. Third Trust Party: TTP

Even if these classical models introduce important concepts that may be interesting in the environment of the CC (e.g. organization, context …), they are unfortunately not fully adapted to this area and have limitations such as:

- The control of activity in the cloud
- Lack of security in terms of quality within the cloud.
- Lack of trust management
- ...

IV. GLOBAL OVERVIEW OF OUR MODEL

Our idea is to develop a model for controlling access to corporate data in a cloud, which will have two main goals. The first is to better control the external connection of users with different accesses (director, manager, HR ...). This situation is well treated by the access control policy applied to traditional and distributed information systems and implies that the company controls the protection of its data that is stored locally. But in the context Cloud, the situation is completely different from that access point and the data are both managed by a third party operator that the company cannot control in any cases. The second objective of our model is to strengthen the confidence of business operators cloud.

To achieve our goal, we first use the concept of Third Trust Party (TTP). A TTP is an entity which facilitates interactions between two parties secures that both trusts in third. We propose in this paper to incorporate the TTP in our access control architecture. In the following sections, we will improve the functions of the third of trusts *TTP*. To do so, we define the following function:

- Set a confidence index of initial trust collaboration with the security manager.
- Decrement the index after each attempt to violate the security policy by the connected user.
- Establish *N* access policies with *PACi (0 < i <= N)* to be managed by *TTP*. These *PACi* change according to a well-defined order.
- The *TTP* switches between a *PACi and PACi-1* following a decrementing the confidence index.

Obviously it is a public policy PACMIN which is the lower limit applied to the general public. For example, a student can connect under a policy *PACi* while the *CEO* will be associated with the broader political *PACj*. A *PACi* policy will no longer be based on the four main modes of access (obligation, recommendation (*cf.* Section V), permission, prohibition), but they will be defined by way of weighted a recommendations with a weight P. This weight is defined in terms of the confidence index, which is connected continuously monitored by the *TTP*. If a user violates one of its rights which have been set, calculating the confidence index varies, then the *TTP* switches from one policy to another more strict. Thus, after malicious attempts or other action relating to trust him, the connected loses all privileges within the company and became a member of the public. In this way, our strategy succeeded in keeping the confidence of the company, and at the same time, do not disconnect the user. Our access control model is therefore based on a set of political variables. These policies are obviously designed by the company itself on the basis of internal confidence.

V. RECOMMENDATIONS

A. Definition

By *controlling* who can (permission), must (obligation), cannot (prohibition) access to data, traditional access control policies and models solve one part of the problem.

In fact, these access modalities does not deal with situations where the system interact with the user by advising him (not obliging him) to do something, and if the user does not follow this advise, he/she assumes the consequences of its action. In this respect, we need an access modality that is stronger than permissions but not very restricting as obligations. Anas Abou Elkalam and al. define this new modality as a "recommendation"[2]. For example, the law [14] gives patients the right to access their medical files, but it recommends that this access be done through the consulting physician (because certain notions in the medical file could be badly understood by the patient, while the physician can understand and present better the situation). The same law stipulates that if in addition the patient is minor or suffers from psychological disorders, it is advisable that he/she be accompanied with his tutor. In fact, we see that this access is stronger than permissions (as the patient assume the consequences if he/she does not respect the recommendation) but not very restricting as obligations (as he/she is not obliged to respect the recommendation). Let us take another example, the Council of Europe Recommendation No. R (97) 5 "on the Protection of Medical Data" [15].

This legislation recommends that medical data shall be obtained from the data subject. It is not an obligation, as it is possible that medical data be obtained from other sources in certain situations (e.g., in particular if the data subject is not in a position to provide the required data). And in the same time, this access is stronger than permission, as the data subject could ask for explanation / justification if the recommendation is not respected, and in certain situations he/she can contest before the judge. We can give several other examples, but due to space limitation we can conclude that security policies in many applications became more and more complex, and there is a great need to find mechanisms to handle the concept of recommendation. This is a big research challenge that was never been addressed. The purpose of the next sections is to present a new model of access control adapted to cloud computing environment.

B. Modeling recommendations

Generally, the choice of a formal language for specifying a security policy is based on the capabilities / richness of this language on the one hand, and on the other hand, on the requirements of the targeted application. In order to specify security policies, we need to express norms, i.e. rules which say what must, may or must not be done. For this reason, in our context, we make choice to base our work on Deontic logic; the latter is able to represent permission (P), obligation (O) and prohibition (F). Actually, Deontic logic [19] is a branch of Modal logic1 [20, 21] that uses permissions, prohibitions and obligations. Typically, if A is a formula and x is a variable in a certain world w, the formula "Ǝx A" means "there exist possible values of x such as A is true in w.

In Modal logic, the "Ǝ" connector can be assimilated to the possibility connector "◊A", and in Deontic logic it is assimilated to the "P (for permission) connector. In this respect, « ◊A or PA » and « A or OA » designate "It is permitted that A" and "it is obligatory that A" respectively. Prohibitions are not forgotten as the formulas « ¬A or FA" express "it is forbidden that A". The formula "◊A " is true in a certain world w if and only if "A is true in at least one of the accessible worlds". Roughly speaking, "◊A" or "PA" means that there exist a possible (at least one) execution of the system where A is true. In the same way, we can deduce that "A or OA" is true in all the possible worlds, i.e., in all the possible executions of the system. Similarly, FA means that A is never possible (in all the possible executions of the system). Now, assume that we need to express rules such as:

- It is recommended to check the certificate in an SSL authentication;
- It is recommended to have the last update of the system;
- Even if researchers have badges to access the laboratory in week-end days, for security reasons, it is inadvisable that a person be alone in the laboratory (a hygiene and safety rule).

In Modal logic, the two notions "it is recommended that A" and "it is inadvisable that B" are represented by the same modality: "◊A" and "◊B". In fact, A as well as B are permitted / possible. We can thus conclude that Modal as well as Deontic logics does not distinguished between what is recommended and what it is inadvisable.

In order to solve this problem, we introduce the "probability of occurrence" notion. In fact, the definition given in the beginning of this section stipulates that a formula A is permitted if and only if there exist a possible (at least one) execution of the system where A is true. According to this definition, the percentage or the probability of its occurrence (in at least one of the possible executions of the system) is not null; we denote this probability by pϵ]0,1].

In this respect, the distinction between "recommended" and "advisable" comes to the distinction between the two following expressions:

- In the possible executions (evolutions) of the system, A could often be carried out;
- In the possible executions of the system, B could rarely be carried out.

By using the "probabilities of occurrence", the notation "◊p A" means "A is possible with the p probability".

When p is not null, "◊pA" is actually permission. Hence, we can deduce that: ◊pA = ◊A if and only if "p# 0".

This is a big research challenge that was never been addressed. The purpose of the next sections is to present a new model of access control adapted to cloud computing environment.

VI. SECURITY POLICIES BASIS OF CONFIDENCE INDEX IN A CLOUD

A. Recommendations weighted

In a comprehensive manner a user can have a succession of policies during his connections to the Cloud from the largest to the strictest. To ensure the finiteness of this result, it is proposed to bring all policies assigned to a user from a point of order allowing these to compare that the policies among each other hi such a way that the above mentioned decreases towards a minimal policy which will keep the user for the rest of his activity on the cloud. Unless the responsible for safety intervenes manually to assign a different policy. To achieve these ends, we introduce an association "*Is_recommended* "type (*Subject, Object, and Action)* and carries a factor "weight". Such that *P ϵ [0, 1]*, to express the fact that a user is recommended to perform an action on an object with a weight P.

This association is represented by the following *UML* diagram:

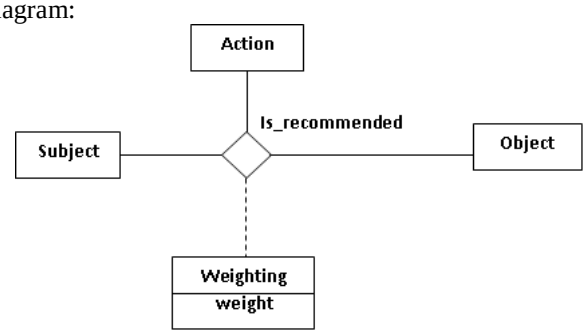


Figure 2: Diagram of the relationship Is_recommended

Properties: Let s be a subject, α action and an object o. Then we have:

- *Is_recommended(s, α, o, 1) <==> is_ mandatory (s, α,o).*
- *Is_recommended(s, α, o, 0) <==>is_prohibited (s, α,o).*
- *Is_recommended(s, α, o, 0.5) <==> is_permitted (s, α,o).*

- P ϵ [0, 1] – {0, 0.5,1} Is_recommended(s,α,o,P) <==> the subject s is recommended to execute the action α on objet o with a weight P.

B. Order of security policies:

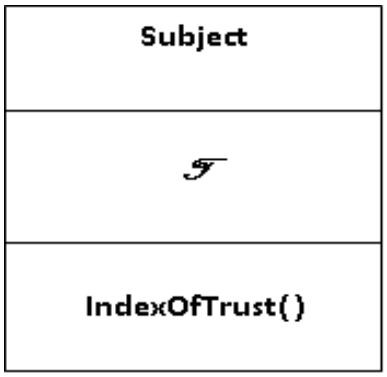
A security policy associated with a user (subject) is the set of recommended actions that can be weighted with this user on objects. Suppose *P1 and P2* two security policies associated with a user at different times during its activity on the Cloud. *P2 <P1 if P2* contains the same actions as P-recommended in *P1* with at least one action with a weight strictly less. We then say that *P2 is stricter than P1*.
Example: *P2<P1*

P1:={ Is_recommended(s, α, o1, 0.4), Is_recommended(s, α, o2, 0.6), Is_recommended(s, α, o3, 0.7), Is_recommended(s, α, o4, 0.8)}.

C. P2:={ Is_recommended(s, α, o1, 0.4), Is_recommended(s, α, o2, 0.3), Is_recommended(s, α, o3, 0.7), Is_recommended (s, α, o4, 0.8)}.

D. Definition of the Trust index $\mathcal{T}$.

We associate with each user (or subject) connected or not, an integer to measure the level of trust granted to him according to his actions on the Cloud. This number will be called confidence index and is denoted in what follows by $\mathcal{T}$. A subject class will have an attribute $\mathcal{T}$ and a method *IndexOfTrust ()* allowing access to this attribute. We represent this class by the following *UML* diagram:



Specifically, at its first connection, each user is assigned a confidence level initial *(T0)* by the security manager, i.e. $\mathcal{T}$ = *T0* at time of first login. If the subject violates the security policy, it is automatically sanctioned by decreasing the one hand his confidence index on the one hand, and by tilting towards a policy of tighter security on the other. If we denote by $\mathcal{T}$n the confidence index of a user at the beginning of its nth connection, then we have:

- $\mathcal{T}_n \leftarrow \mathcal{T}_{n-1}$ with $\mathcal{T}_1 = T0$
- $\mathcal{T}_n \leftarrow \max(\mathcal{T}_n - S, 0)$ if the user violates the security policy in this connection. The integer S is the penalty for this violation.

This evolutionary process of the confidence index stops when it reaches 0. In this case, the associated security policy is automatically logged on to public policy (policy and minimum designated by PMIN granted to any user).

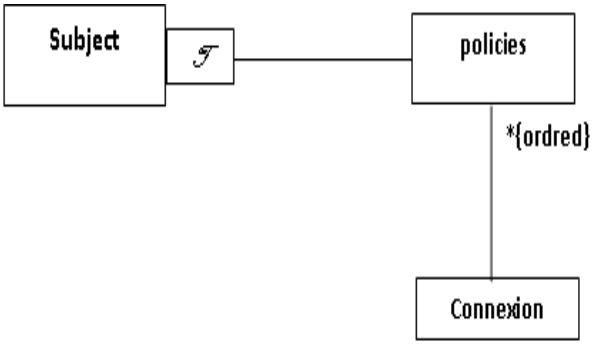


Figure 3: Relationship diagram

E. Calculating the value of the penalty

In the cloud environment, the company requires a degree of confidence sufficient to deport its data to an operator cloud. This degree is strongly linked to the user having a right of access to corporate data. Hence the importance of establishing a control mechanism of a confidence factor $\mathcal{T}$ of each user. This control will decrement $\mathcal{T}$ by a sanction S. Recalling that $\mathcal{T}$ is essentially based to control and modify the rights of each user connected. This change is reflected as a sanction S defined above. The calculation of S considers several parameters:

- **Basic trust *T0*:**

The security manager assigns a confidence about when creating accounts and sessions. The connected must ensure that T0 is constant (this setting down for violations of the policy) during the connection because the value of the initialization may depend on the change curve of the confidence index initialized by T0, where T0 = confidence affected by the security manager.

- **Number of malicious attempt NMA "Number of malicious actions":**

Management malicious actions within the cloud are the most important part of our article. Indeed, the implementation of the coefficient allows *NMA* attempts to control human rights violations before the actual violations. Sanctions generated by incrementing the *NMA* are within the heart of our access control model *TOrBAC* "see section 4". This parameter is an integer initialized to zero when creating the account, it is incremented (by 1) after each non-compliance with the policy (e.g. malicious attempts). Obviously, after each attempted rape of politics, that *T0* decreases by a positive step. This sanction is not related only to NMA but also to the frequency of connection and disconnection. Hence the need to introduce meters in this direction.

- **Connection counter NC**

The frequency of a user logs, indicates more information on the identity of the connected, when we compare this number with the normal average of these needs. This is an integer initialized with zero and incremented (by 1) after each connection. This number can bring several information that facilitates in their turn the trust management in as a broad environment such as Cloud. This counter is still very useful when combined with that of the disconnection.

- **Counter disconnection ND**

This is necessarily an integer less than or equal to N in normal cases. It counts the number of closures correct session; its importance is that to compare it with NC, so for a user who meets the security policy, the NC is equal to *ND or NC=ND+1* in or if he is offline. In other words, if the *NC > ND + 1 + K, where K> 0*, then we can deduce that the system has already forced the disconnection of this user K times, after a period of idle connection. This behavior deserves punishment naturally, hence the interest to include in the calculation of our confidence level.

- **Duration of passive connection DPC "Duration of passive connection"**

The passivity of a session is normally not recommended in the cloud environment by it touches the confidentiality of data to which it is entitled access. This is an index that reflects the carelessness of the user. This behavior can affect the confidentiality of information because it opens a window through this session, through which a person can do a consultation. This coefficient will link the logon necessarily to a continuous activity and legal identity connected. The penalty generated by this behavior is translated via the number of times or the disconnection of the session is forced. Note *NDPC* as an integer that will be part of the definition of our confidence index.

Our idea is to generate a sanction S according to: *NMA, NC, ND and NDPC. With S ϵ [0, T0]* which is a step of decrement the T. Thus, we define the value of S as follows: *S = (N-ND) * (NMA + NDPC).*

Properties:

a) This decrement is running:

- *Real time*:

- If NDPC is incremented after the expiration of the predefined maximum time of passivity.
- If NMA is incremented after registration of an attempted violation of any rights of the user.

b) T converges to zero.

c) The speed of convergence depends on the degree of tolerance adopted by the security policy of the owner of the service (data, software ...).

(d) If ND = NC then the connection is idle when the index of T is zero.

So we set the penalty to be generated for all users who touched the trust settings. In the next section we explain the actors who manage these sanctions.

F. The Management Security Policies By Relying Party (TTP) based on the confidence index T

In a cloud field design policies Pi is much broader than the information system *(IS)* distributed classic. It is in this light that OrBAC can open an important avenue to design a model adaptable to the cloud. We can therefore design policies embedded in a sense of inclusion of P-recommendations, as an extension of the model proposed by Abu Anas Elkalam et al. [2]. This set of policies will be managed by *TTP (Trust Third Party)* by the mechanism of Figure 4, depending on the confidence index sets $\mathcal{T}$ in the previous section.

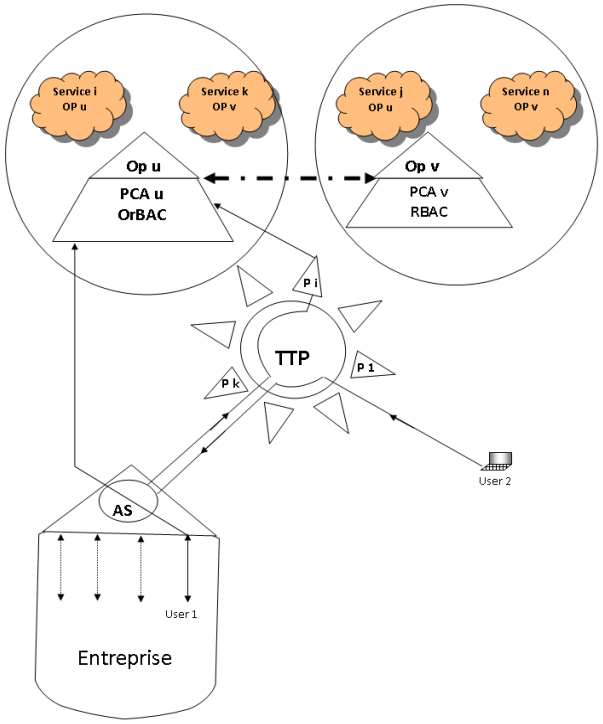


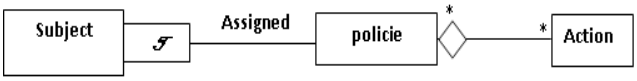
Figure 4: Access control architecture for trust.

In our architecture, a *TTP* must ensure compliance with security policy given to each subject connected. It monitors its actions in cases of rape and policies (e.g. illegal action), *TTP* decreases its confidence index and replaces its security policy by running a new stricter. The user can then go through a succession of security policies *(P1, P2, ... PMIN) ≤ P with Pk <Pk-1..... <P2 <P1.*

At every moment, a user has a confidence and a single security policy. Any change in the first one will automatically change the second. Relationship is used Assigns type *(TTP, Subject, Policies)* to model this statement:

Assigns (TTP,s,P) means that *TTP* assigns policy *P* on subject s.

It schematizes this ugly relationship to the UML diagram below:



Subject (s) + IndexOfTrust (T) ===> a policy of security (P)

This relationship can be formulated in first order logic as follows:

∀ S ∋! T ∋! P such that T =IndexOfTrust(s) and Assigns(TTP,s P).

Now to model the role of a *TTP* in a cloud environment, we define two new relations and Control Changes of type (*TTP, Subject*) and (*TTP, Politics, Subject*) respectively:

- *Control (TTP, s)* means that *TTP* monitors the actions of the subject's activity of s in the cloud.

- *Modifies (TTP, P, s) <===> Control (TTP, s) AND IndexOfTrust(s) down AND if there is a policy P 'as PMIN <P' <P Assigns AND (TTP, s, P ').*

We illustrate this relationship in the *UML* diagram below (Figure 5):

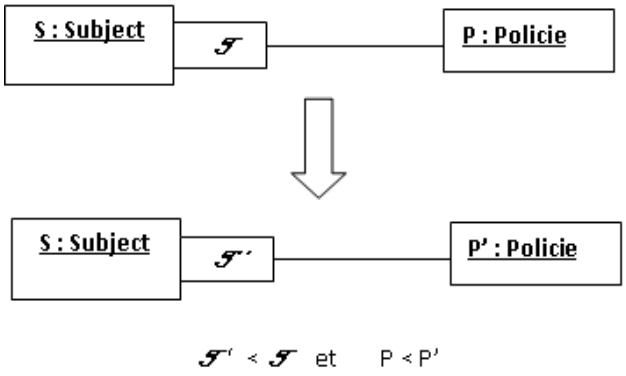


Figure 5: Object diagram describing the rocking of a policy P to another policy P '.

It finally gives the class diagram below illustrates the relationships between different classes Subject, Connections, Connection, *TTP*, Policy and Actions:

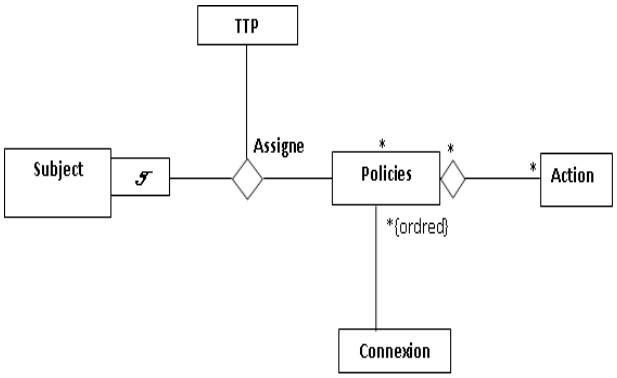


Fig 6: Main diagram of different relationships.

Control the relationship, defined in Figure 5, indicates that *TTP* alters the confidence index of a subject acting on actions that have been allocated. For example if a member of a university hospital tries to view the information which he has no right, *TTP* augment the *NMA* and *therefore* its T *decreases*.

G. Architecture of Model TOrBAC

Now that we have defined the principle of access control based on the confidence index, and we extended the right of access to *P-recommendations (weighted)* with *0 <= P <= 1*, instead of permission, prohibition and obligation. We can integrate the dynamic relationship between identity (state trust) and rights attributed to him. Our model, as shown in Figure 7, based on the recommendation with a weight weighted P to an activity by a subject s org or dependent: the cloud environment and the confidence index $\mathcal{T}$ *(real time management by the TTP).* Thus if s is a subject, a view v and a context c then *Is_recommended (s, α, o, P)* means that subject is recommended (*in the order P = TTP* ($\mathcal{T}$)) to perform the action α o on the object. Obviously, with this architecture can implement counter measures to mitigate malicious activity in the Cloud without compromising their connections.

For example in a universal virtual meeting; within a federation of n *CHU* (*university hospitals*) whose objective is to find a solution for a case with a complicated medical history. In this environment the federation recommends that *P = 0.5* to a doctor each *CHU*, consult the medical diagnosis part of the record for possible collective solution. But if one of these doctor tries to see the plaintiff's case, his confidence level $\mathcal{T}$ decreases and loses the case in remaining as an observer in the meeting. We cannot enter in this article in full development of the specification of security policies based on trust management in a cloud of *CHU*. We present only some examples of how to monitor and react to the $\mathcal{T}$ index of such organization or subject.

Our model is highly useful for an integration of several teaching hospitals in the world *(CHU1, CHU2, ...)* with laboratories that interact in real time *(LAB11, LAB12 ...., Lab21, LAB22 ....).* Thus we have such symbols as constants Environment private cloud, cloud community, Cloud hybrid etc.. ; Confidence index *T ϵ [0, T0]*, as *CHU1 Organization, CHU2* etc, constant symbols of type Subject like physician1, medecin2, CHU1, etc.., The constant symbols of type Object as *FICH1.doc, file2. doc, FICH3.tex*, etc.; Shares as read, write, consult, etc., the constant symbols of type Role as *Unit1, Unit2, LABO11, LABO21*, etc.; constant symbols of type view as the administrative record, consulting, attending Vital cased judicial-record, and; constant symbols of type activity like reading, writing, consulting, etc..

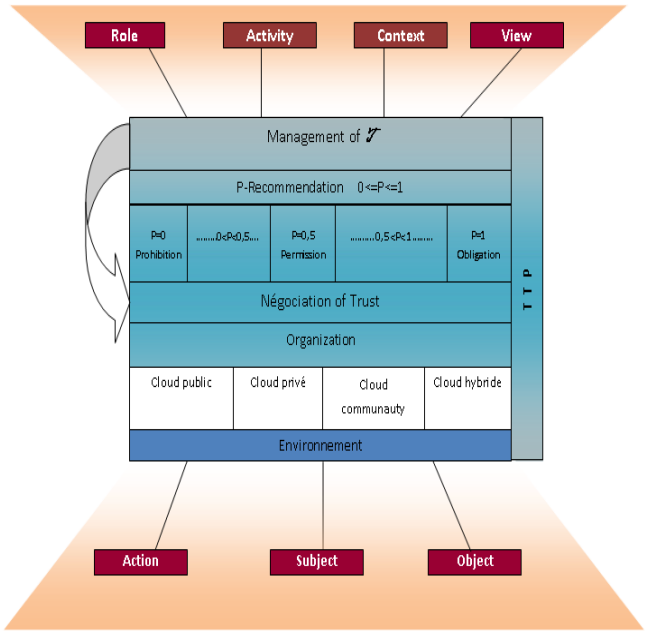


Figure 7 : Architecture Model TOrBAC.

VII. CONCLUSION

This paper introduced and explained the definition of Cloud Computing (CC) environments, including associated concepts, architectures, infrastructures, deployment modes as well as its specific security risks and threats. We then explain that access control models and authorization systems in the CC are of vital importance as they specify and formalize who has access to what in this complex environment. Models like RBAC and OrBAC are interesting but needs some extensions to be able to cover all the CC security requirements. We thus presented in this paper the Trust Organization Based Access Control model (TorBAC).

This model takes into consideration the management of trust in the environment via the Cloud Comuting function of TTP and parameters confidence indicators.

This work can be extended to a model encompassing the deeper mechanisms of detection of rape in the cloud environment. In our future research we focus on the relationship between trust and reputation for service quality within the Cloud. All these ideas are useful to extend the InterCloud promises to be a normal extension of the cloud. Finally, we expect applying our results to a more realistic use case and developing the associated mechanisms to verify the consistency and completeness of the security policy.

REFERENCES

1. A. Abou El Kalam, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, R. El-Baida, A. Miège, C. Saurel, G. Trouessin "Organization-Based Access Control", 4th International Workshop on Policies for Distributed Systems and Networks (Policy'03), Côme, Italie, 4-6 june 2003, IEEE Computer Society Press, pp. 120-131.
2. A. Abou El Kalam, "A Research Challenge in Modeling Access Control Policies: Modeling Recommendations", IEEE International Conference on Research Challenges inInformation Science, 3-6 Jun 2008, Marrakech, Morocco.
3. Anas Abou El Kalam, Yves Deswarte, Amine Baina, Mohamed Kaaniche, PolyOrBAC: a Security Framework for Critical Infrastructures, Rapport LAAS N°09087, 28 pp., International Journal on Critical Infrastructure Protection, Elsevier, vol. 2(4), Decembre 2009, 37pp, LNCS.
4. DomBAC: An access control model for moder collaborative systems Antonios Gouglidi s *, Ioannis Mavridis Department of Applied Informatics, University of Macedonia, 156 Egnatia Str., 54006 Thessaloniki, Greece
5. TBAC : R. Thomas et R. Sandhu. Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management. 11th IFIP Working Conference on Database Security, Lake Tahoe, California, USA, 1997.
6. RBAC : ESEP 2011: 9-10 December 2011, Singapore Role-Based Access Control Model of Cloud Computing Chen Jincui and Jiang Liqun China University of Mining and Technology, Xuzhou221008, China
7. www.ORBAC.org
8. ESEP 2011: 9-10 December 2011, Singapore Role-Based Access Control Model of Cloud Computing Chen Jincui and Jiang Liqun China University of Mining and Technology, uzhou221008, China
9. A. Abou El Kalam, P. Balbiani, "A Policy Language for Modelling Recommendations", IFIP TC-11 International Information Security Conference, (IFIP SEC 2009), Cyprus, 18-20 juin 2009, Springer.
10. Livre Cloud : Cloud Computing - 2ème éd - Une rupture décisive pour l'informatique d'entreprise : Guillaume PLOUIN.
11. Livre blanc MIBS et Pierre Audouin Consultants : " Les infrastructures critiques : bien maîtriser le socle du patrimoine informatique de l´entreprise " .
12. Recent Advances in Cloud Security Jiyi Wu 1,2 1.Key Lab of E-Business and Information Security, Hangzhou Normal University,Hangzhou,China 2.School of Computer Science and Technology, Zhejiang university, Hangzhou, China & al.
13. Luo et al. 2011, C.L., A hierarchy attribute - based access control model for cloud storage, in Proceedings of the 2011 International Conference on Machine Learning and Cybernetics (ICMLC), vol. 3, pp. 1146 - 1150, IEEE, 2011.
14. Law 2002-303 related to the patient's rights and to the quality of healthcare systems, Article L. 1111-7, March 2002.
15. Recommendations of the Council of Europe, R(97)5, On The Protection of Medical Data Banks, Council of Europe, Strasbourg, 13 February 1997.
16. Book: Cloud Computing Bible : Author: Sosinsky, Barrie Edition: John Wiley & Sons Publication: 2011.
17. Livre blanc : Quelles tendances pour le Cloud Computing en 2011 ?
18. Livre blanc produit par Euro Cloud France November 2011.
19. J.I. Andrew Jones, J.S. Marek, "On the Characterization of Law and Computer Systems: The Normative Systems Perspective." In John-Jules Ch.Meyer and Roel J.Wieringa, Deontic Logic in Computer Science: Normative System Specification, John Wiley and Sons, Chichester,England, 1993.
20. B.F. Chellas, "Modal Logic: An Introduction", Cambridge University Press, 1980, ISBN 0-521-29515-7, 295 pp.
21. S. Kripke, "Semantical Consideration in Modal Logic", Acta Philosophical Logic, vol. 16, 1963, pp. 83-94.
22. R. Sandhu, D.F. Ferraiolo, D, R. Kuhn (2000), "The NIST Model for Role Based Access Control: Toward a Unified Standard," Postscript PDF Proceedings, 5th ACM Workshop on Role Based Access Control, July 26-27, 2000, Berlin, pp.47-63
23. [Abou El Kalam & Deswarte, 2009b] A. Abou El Kalam, Y. Deswarte, "Poly-OrBAC: An Access Control Model fior Inter-Organizational Web Services", Handbook of Research on Semantic Technologies and Web Services, ISBN: 978-1-60566-650-1, May 2009, IGI-Global Editor,
24. <http://www.igi-global.com/reference/details.asp?ID=34405>
25. [Abou El Kalam et al. Cloud Computing - 2ème éd - Une rupture décisive pour l'informatique d'entrepriseInternational Journal on Critical Infrastructure Protection, Elsevier, vol. 2(4), Décembre 2009, 37pp, LNCS.

AUTHARS PROFILE

Mustapha Ben Saidi Checheur security of information. In University Hassan I Morocco.holds a degree in higher education and telecommunications networks. Member of the association AMAN Morocco. His current research interests are Software Engineering, Software Security and Software Process Modeling adapted to Cloud computing.

Dr. Anas Abou El Kalam is the President of the Moroccan Association of Digital Trust (AMAN: Association Marocaine de confiAnce Numérique). He is a professor at the UCA-ENSA and the head of the "Network and Telecommunication department"; he is also in charge of the "Networks, Systems and Security" master. He was an associate professor at the "Institut National Polytechnique" (INP) of Toulouse – France where he also obtained his HDR (Habilitation à Diriger les Recherches) in "security of critical networks and systems" as well as his PhD in "security policies and models" (at the "Laboratoire d'Analyse et d'Architecture des Systems (LAAS-CNRS)"). He had several responsibilities as the Head of the "Computer Science Department" and the head of the "Networks and Systems security" Department at ENSIB – France. He is the PC Chair of several conferences such as the IEEE International Conference on Risks and Security of Internet and Systems (CriSIS) and the National Security Days (Journées Nationales de la Sécurité). He is/was a member of the programme committees of several prestigious conferences on security such as IEEE ACSAC (Annual Computer Security Application Conference), SECRYPT (International Conference on Security and Cryptography), IFIP SEC (International Information Security Conference), ESORICS, WSCN, CMS, etc. He participates to several Airbus projects (such as Aircraft Data Communication Networks "ADCN" and Information management for Avionics Platforms "IMAP") as well as several European projects such as FP6/IST PRIME, FP7/IST CRUTIAL, NoE Newcom++, Celtic Fell@home. His current research interests concern security of embedded systems, network security, wireless security, security models and intrusion detection systems. He has authored 20 book chapters and ineternational journal papers as well as more than 90 international peer reviewed publications. He has been security consulting for several European companies and a security expert (evaluator) for the French National Research Agency (ANR) since 2009.

Dr. Abderrahim Marzouk received his Ph.D(Computer Science) from University of Cean (France) in 1995. He has more than 15 years of experience in teaching Computer Science, JEE Technology and Web Applications. His current research interests are Software Engineering, Software Security and Software Process Modeling (UML, XML, OWL).